Securing WSO2 Private & Public Clouds

Version 1.0

Date: November 2022

Inquiries: security@wso2.com

Correspondence: WSO2 Inc.

Table of contents

Overview

With the introduction of Kubernetes-Native WSO2 Public (Asgardeo & Choreo) & Private Cloud deployments, we introduced DevSecOps practices to our Software Development Life Cycle (SDLC). It also changed the culture, process and tools across all our core functional teams and made security a shared responsibility among all. We have integrated security tools into Continuous Integration and Continuous Deployment (CI/CD) pipelines wherever it is possible to automate the scanning process.

We have divided this document into multiple sections to explain what secure design patterns and security controls we have deployed into our public and private cloud deployments to protect against major threats like Internal attacks, Software Supply Chain attacks, Employee account takeover, Service and Platform attacks etc.

Compliance

With WSO2's ever-increasing global footprint, the group has commenced several Governance and Compliance initiatives, focused specifically on the cloud environments.

SOC 2

WSO2 is currently in the process of obtaining the SOC 2 Type 2 compliance (Security, Confidentiality & Availability Trust Service Criteria) for WSO2 Public Cloud Offerings (Asgardeo and Choreo) & Private Cloud Offerings. SOC 2 Type 1 report would be available by the end of Q1 2023, and SOC 2 Type 2 report would be available in Q4 2023.

If the customer is considering the **Public Cloud offering** then they could leverage the SOC2 compliance once we complete the audits. Please note Private Data Planes are excluded from the SOC2 scope.

If the customer is considering the **Private Cloud offering** then there needs to be a separate engagement with the WSO2 DevOps team. A separate deployment would be created on behalf of the customer with relevant security controls in line with SOC2 requirements and audited by the SOC2 auditor in upcoming audit cycles. Auditors do require live production data for a period of 6 months prior to doing such attestations.

ISO 27001:2013

ISO 27001:2013 is a global standard for information security. Currently, WSO2 Digital Operations is certified on this standard. With WSO2's increasing cloud presence, the scope of this certification would be extended to include cloud operations, thereby enhancing our security practices while giving added assurance to our customers and other stakeholders.

We also plan to incorporate controls from the ISO 27018:2019 standard (Privacy in Cloud environments) and the ISO 27017:2015 (Security in Cloud environments) standard for added security and assurance.

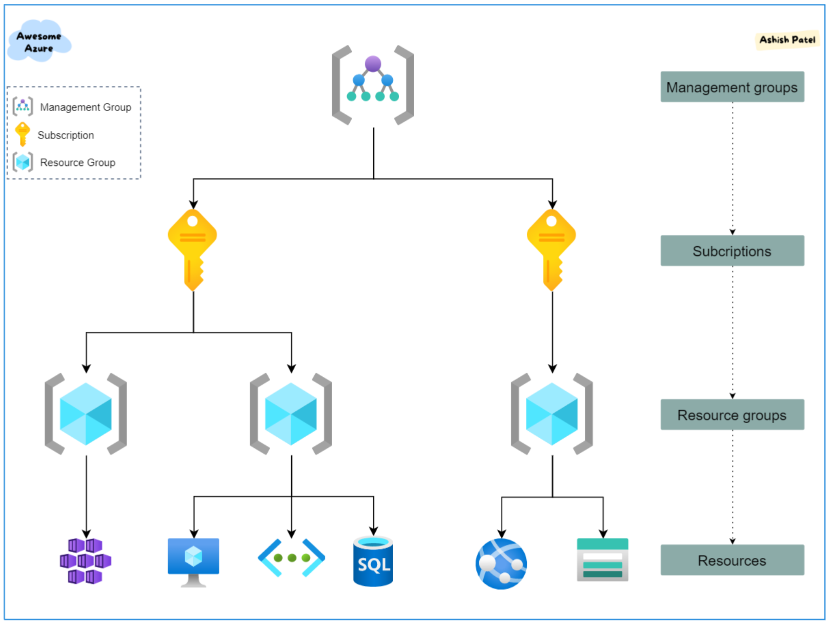
Other Initiatives

Key compliance initiatives included in our roadmap include

a) SOC 2
b) FedRAMP
c) CSA STAR Levels 1 and 2

Cloud Governance

WSO2 is using Azure as our primary public cloud service provider to host our cloud offerings. (AWS and GCP are also in the pipeline). We use Azure Management groups and Azure subscriptions to logically segregate our environments. We use Azure Policies to enforce control over management groups and subscriptions.

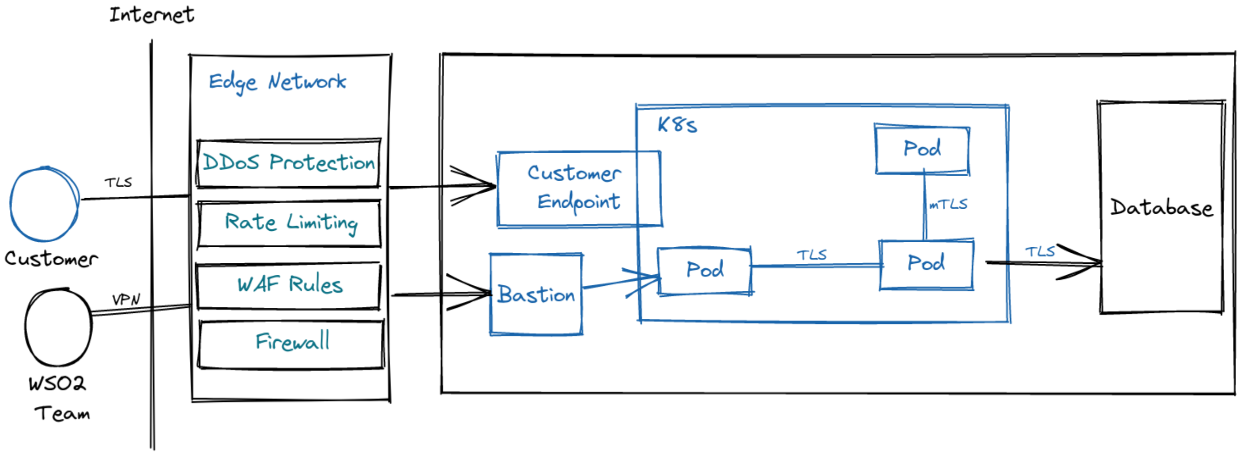


Identity & Access Management

Azure AD Identity Protection identifies and blocks risky Azure sign-ins. Our Security Operations Center (SOC) monitors any alerts generated by unusual user logins and takes prompt actions.

We follow the Least Privilege and Role Based Access Control (RBAC) Model to grant permissions to cloud resources. We have enforced Multi-Factor authentication (MFA) and Privileged Identity Management (PIM). Users are authorized via PIM for administrative tasks. Further, we are performing User Access Reviews using automated scripts.

Network Security



Network security is an integral element in the runtime security aspect of all WSO2 cloud offerings. Its defense-in-depth strategy brings in zero-trust and threat-based controls to provide optimum security for the network at:

Inbound connections

All external network connections reaching WSO2 cloud infrastructure are expected to be either TLS encrypted or via a VPN route to avoid man-in-the-middle attacks.

All public endpoints are DDOS protected and rate-limited.

All inbound connections are tunneled to the internal network via an L7 firewall with IDPS, and threat intelligence is enabled. In the cases of web application traffic, the same is tunneled through a Web Application Firewall (WAF) to secure the internals from incoming attacks.

All direct interactions with the internal infrastructure are via a secure bastion resource.

Internal network and connections

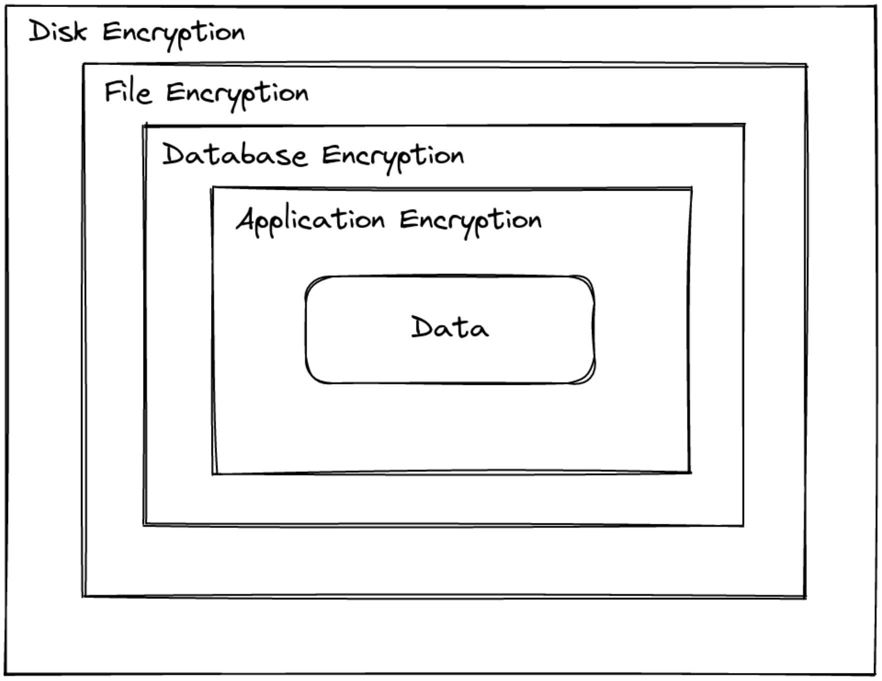
Internal Network Access Controlling between cloud resources are achieved through network security groups. The same among containerized cloud workloads is achieved through Kubernetes network policies.

All internal connections are expected to be encrypted; in some scenarios, this is achieved by enforcing mutual encryption using a service mesh.

Outbound connections

All outbound connections to the outside are also tunneled through an L7 firewall with threat intel for malicious IPs / domains and IDPS being enabled.

Data Protection



Deployment specific controls:

- Data at rest is encrypted with AES-256.
- Data in Transit is encrypted with TLS 1.2 or above.
- WSO2 is using Azure Key Vault to securely store all secrets in Public and Private Cloud environments.

Detection & Response

Public Clouds

WSO2 Public Cloud offerings are monitored by our security Operations Center (SOC) for security incidents and anomalies.

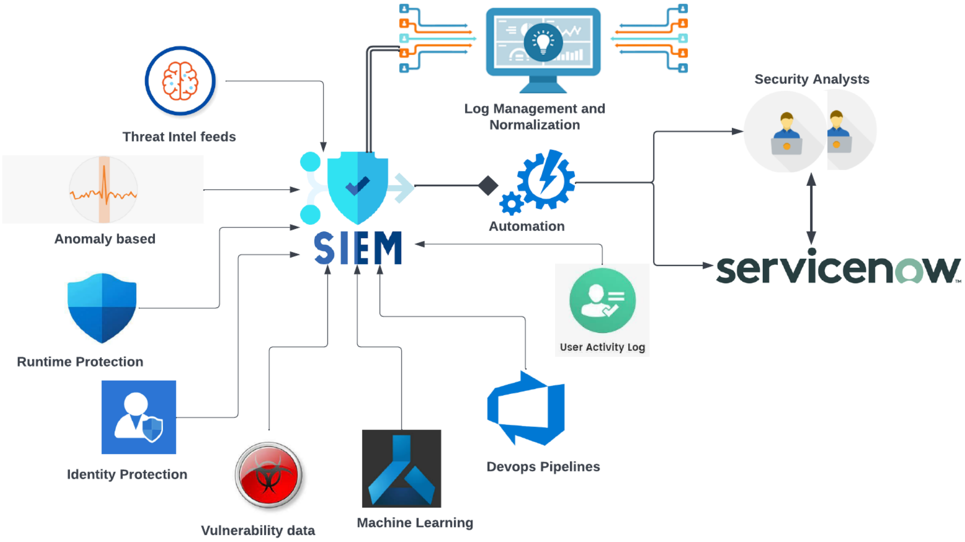
WSO2 follows a well-defined resource onboarding process where integration with the central log management solution would occur to ensure all production resources are covered by the central Security Incident and Event Management (SIEM) solution.

The following detection types are currently used in WSO2 cloud offerings,

- Anomaly-based.
- Threat Intelligence-based.
- Vulnerability based.
- Custom threat parameters based.
- Runtime protection.
- Machine learning capabilities powered by Microsoft.

The threat detection scope is not limited to resource types but extends to

- Azure Identities.
- Development pipelines.
- User activities



WSO2 Cloud Security detection and response strategy

WSO2 follows well-defined processes in line with industry standards and best practices on Incident Management, Vulnerability Management, Patch Management, Change Management, etc. to handle security incidents.

There are several channels established to report security incidents.

All reported incidents will be recorded in the centralized ticketing system (ServiceNow) and tracked until closure.

Other than reactive actions, WSO2 is highly focused on proactive and continuous threat-hunting activities.

Private Clouds

WSO2 Private Clouds are currently not monitored by the SOC team.

As per the customer’s requirement, detection alerts can be configured and integrated with the customer's Security Operations Center or any preferred monitoring mechanism. Further WSO2 team can provide recommendations to implement detection and response use cases in the Private clouds.

Kubernetes Security

Kubernetes security is vital for WSO2 as most application workloads run on WSO2 cloud infrastructure are containerized and use Kubernetes as their container orchestration platform. To achieve optimum security, both zero trust and threat-based security controls are in place as follows.

Zero trust security controls:

1. Kubernetes RBAC is in place with a well-reviewed process of permission assignments to users and service accounts.
2. All container workloads are sandboxed with Seccomp and AppArmor security profiles to restrict unwanted Syscalls and resource access of nodes.
3. After performing authentication and authorization checks with Kubernetes RBAC, all container workloads are verified using admission control policies for secure configurations of users, privileges, capabilities, etc.
4. Kubernetes network policies currently achieve network segmentation and control.

Threat-based security controls:

1. Intrusion detection at Kubernetes cluster level, node level, and container level (privilege escalations, process, file access, and network related) is currently taken care of by Azure security technologies supporting eBPF.
2. A central Firewall handles intrusion detection at the network level, which effectively performs IDPS and threat intelligence at L3 / L4 and L7. In the cases of inbound web application traffic, a WAF is in place to detect malicious application-level activities.

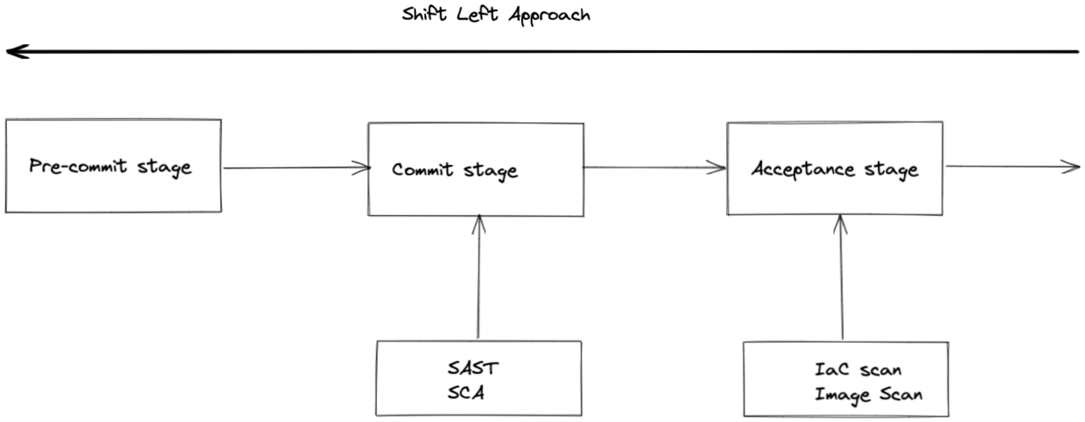
Vulnerability Management

CI/CD Pipeline Scanning

To secure the applications, services, and other software running on our cloud solutions from existing and zero-day security threats and vulnerabilities, we have integrated scans throughout our CI/CD pipeline. It includes Static Application Security Testing (SAST), coding best practices, and Software Composition Analysis (SCA).

In the shared responsibility model, our cloud service provider is responsible for building upgraded Kubernetes node images, and we are responsible for updating the nodes with the latest images. We continuously upgrade our Kubernetes clusters to apply the latest patches and updates.

At the same time, we scan the rest of the images we deploy in our clouds for vulnerabilities at the OS level, application level, and third-party dependencies before admitting them to our environments.



CICD pipeline

Cloud Security Posture Management

We use Microsoft Defender for Cloud Security Posture Management (CSPM) capabilities and tools to gain visibility of our cloud security and compliance posture. It helps us to understand risks and mitigate them. In addition, we closely monitor the secure scores and identity scores of our private and public cloud subscriptions and take continuous actions to increase both scores.

We identify the misconfiguration issues in our Infrastructure as Code (IaC) in multiple places throughout the CI/CD process.

- IDE level scanning/Scanning at the developer machine
- Scan before merging the pull requests
- Scan before releases.